

09/711,323

OCT 14 2008

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS

1. (Previously Presented) A method for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by the intrusion detection system, the method comprising the steps of:
 - (a) transmitting to the first sensor information about a belief state of the second sensor, said belief state of the second sensor indicating a state of at least one system resource or service directly monitored by the second sensor; and
 - (b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a state of at least one system resource or service directly monitored by the first sensor, the adjusting based at least in part on the belief state of the second sensor, so that a sensitivity of the first sensor to suspicious activity in the intrusion detection system is improved.
2. (Previously Presented) The method of claim 1 wherein the first sensor and the second sensor are different types of sensors.
3. (Original) The method of claim 2 wherein the first sensor is a probabilistic sensor.
4. (Previously Presented) A method for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by the intrusion detection system, the method comprising the steps of:
 - (a) transmitting to the first sensor all or part of a belief of the second sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored by the second sensor; and

09/711,323

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating an apparent normal, degraded or compromised state of a resource directly monitored by the first, so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system.

5. (Previously Presented) A method for enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of a belief state of the second sensor regarding an existence or validity of services supported on computer system resources directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating an existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious to the intrusion detection system.

6. – 9. (Cancelled)

10. (Previously Presented) A computer readable storage medium containing an executable program for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor information about a belief state of the second sensor, said belief state of the second sensor indicating a state of at least one system resource or service directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a state of at least one system resource or service directly monitored by the first sensor, the adjusting based at least in part on the belief state of the second

09/711,323

sensor, so that a sensitivity of the first sensor to suspicious activity in the intrusion detection system is improved.

11. (Previously Presented) A computer readable storage medium containing an executable program for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by of the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of a belief of the second sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating an apparent normal, degraded or compromised state of a resource directly monitored by the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system.

12. (Previously Presented) A computer readable storage medium containing an executable program for enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of a belief state of the second sensor regarding an existence or validity of services supported on computer system resources directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating an existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious to the intrusion detection system.

13. (Cancelled)